

# A Detailed Analysis of Trust Representation as a Trust Model Evaluation Criterion (May 2006)

M. Wojcik<sup>1</sup>, H.S. Venter<sup>2</sup>, J.H.P. Eloff<sup>3</sup>

hibiki<sup>1</sup>@tuks.co.za  
{hventer<sup>2</sup>,eloff<sup>3</sup>}@cs.up.ac.za

Information and Computer Security Architectures Research Group  
(ICSA)  
Department of Computer Science  
University of Pretoria

**Abstract—** Technology and the advent of the Internet have resulted in an environment that is both dynamic and changing. This dynamic environment has resulted in the need for trust establishment between agents that have not previously interacted before. In order to address this need, trust models have been proposed in order to handle the establishment and evaluation of trust. Trust models rely on logical rules to analyze the nature of interactions between two agents. An agent in this context is usually a computer running a trust model, analyzes other agents it comes into contact with and determines a trust level.

However, due to the novelty of the subject matter, the trust models currently proposed are wide and varied. Currently, there is no common set of features that have been standardized throughout trust model implementation and no means of evaluating various trust model implementations exists. This paper proposes a set of criteria that is to be used to evaluate various trust models in order to identify the specific trust-based issues addressed by a particular trust model. Four main categories into which these criteria fall, have been identified. Due to space constraints only one of these categories is discussed in detail followed by an example analysis of a trust model in order to illustrate how these criteria are used for trust model evaluation.

**Index Terms—** Trust, criteria, trust model, trust representation

## I. INTRODUCTION

Trust and the intricacies thereof has been a topic of interest in disciplines such as sociology, psychology, economics, philosophy and even history [1]. The advent of the Internet and e-commerce has triggered a similar interest in the concept of trust within the discipline of Computer Science. This new environment provides a wealth of new opportunities for gathering information, providing new services and participating in business interactions. However, in the same way that this environment provides new opportunities, it also exposes the participants to new levels of risk. With the existence of risk comes the need for trust.

The dilemma that emerges in the field of Computer Science is that of defining trust among agents that may not have interacted before. Interacting within a dynamic environment such as the Internet allows agents that may not have interacted before to interact with one another. In order to somehow manage the risk that comes from interacting with unknown nodes, a means of defining trust is required.

Several experts in the field have defined trust models in order to allow agents within a computerized environment to establish trust [2], [3], [4], [5]. An agent in this context refers to a computerized agent that has some form of trust mechanism in place. However, the models that have been proposed are wide and varied, each focusing on different aspects of the trust building process.

The problem with all these wide and varied models is that there is no consistent set of criteria that is upheld throughout making it difficult for an interested party to decide upon a particular trust model to implement. This paper attempts to solve this problem by introducing a set of criteria that can be used to analyse a given trust model. Another goal of this set of criteria is to allow for easy identification of possible lack in current trust model architecture and to assist in guiding the development of future trust models by defining what is required. The criteria, as defined by the author, consist of four main categories which contain various

---

This research is funded through the Centre of Excellence in Teletraffic Engineering for the Information Society (CeTEIS), Telkom SA Limited. Any opinion, findings and conclusions or recommendations expressed in this material are those of the author(s) and therefore Telkom does not accept any liability thereto.

influencing factors contained within. These four categories are trust representation, initial trust, updating trust and trust evaluation. Due to space constraints only trust representation is discussed in detail.

The remainder of this paper is structured as follows. The background, section II, explores the concept of trust and how it is currently formalized by experts in the research field of trust models. Section III defines the set of criteria that is to be used to analyse a given trust model. A basic analysis is given in section IV to illustrate the means in which this criteria is used. Finally, the discussion and conclusion of this paper occurs in sections V and VI respectively.

## II. BACKGROUND

Trust models rely heavily on the concept of trust, often modelling human psychological ways of forming, establishing and maintaining the concept. In order to fully understand trust model architecture it is important to first explore and define the concept of trust. This section explores the concept of trust and introduces some work already done in the research field of trust models.

### A. Trust

Trust is such an intricate part of our daily lives that we use it constantly without even thinking about it. However, a clear definition has been hard to come by mainly because trust is a unique concept to each individual influenced by one's own beliefs, morals and experiences. It is thus accepted that trust is subjective.

Nooteboom [6] defines trust as a four-place predicate stating that: "Someone has trust in something, in some respect and under some conditions." These predicates refer to: the agent trusting (someone), the agent being trusted (something), the reason and goals that define the need for trust (respect) and the conditions under which the trust is given (conditions).

This definition can be further expanded by including Golembiewski and McConkie's [7] views on uncertainty and hopefulness. With uncertainty comes risk. Without the existence of uncertainty there would be no need for the concept of trust as the outcome will be pre-determined. In essence, in order to trust, one has to be willing to submit to the risk that the trust may fail, but expecting that it will not. Trust does neither guarantee success nor does it give a failsafe method of analyzing interactions. Without risk, trust does not exist [6].

Trust is a dynamic concept that changes over time depending on the experiences and situational factors that influence the formation thereof. Many situational and cognitive factors influence the formation of trust among humans. These factors include concepts such as reputation, recommendation, observation and experience. Since humans build on the concept of trust, these factors are also found among computerised trust model definitions.

### B. Trust Models

Several trust models have been proposed by various experts in the field. These models focus on various aspects of the concept of trust. Various computing environments

present various challenges when considering trust formation. Establishing trust in the environment of ad-hoc networks is explored by Pirzada and McDonald [8]. Pirzada and McDonald approach the formation of trust in such an environment from a more passive perspective by allowing agents to observe one another in passive mode before attempting to participate in any interactions. Information is gathered through analysis of forwarded, received and overheard packets. Certain events are recorded, categorized and analysed in order to obtain a trust evaluation.

Pirzada and McDonald's trust model illustrates the formation of indirect trust requiring agents to form trust before interacting with another agent. Trust can also be established directly by allowing direct interactions with an agent in question. A means of establishing a direct trust is formalized by Jonker and Treur.[9]. Jonker and Treur define a trust evolution function by using a mathematical function to formalize the influence of past experiences on the level of trust; whereby sequences of experiences are converted into trust representations.

These are but a few of the trust models that have been proposed. It is clear that these models are varied, concentrating on different aspects of trust. Finding a commonality and structure among various trust models is often difficult if not impossible. This makes it difficult for an interested party to choose a trust model that best suits specific needs. This paper addresses this problem by defining a set of criteria anyone interested in trust model implementation can use in order to determine a trust model's efficiency.

## III. CRITERIA FOR EVALUATION OF TRUST MODELS

Basic trust model architecture can be defined by four broad criteria by which trust models can be evaluated, as defined by the author. These criteria include trust representation, initial trust, updating trust and trust evaluation. Trust representation looks at how a trust model represents trust-related data. Initial trust defines how a trust model obtains an initial trust value for a node it has previously not interacted with while trust update allows a trust model to dynamically update a trust value over time. Initial trust and updating trust are closely linked as usually the means in which initial trust is obtained, is usually carried through to the means in which it is updated. Finally, trust evaluation looks at various influencing factors on the trust evaluation process. Due to space constraints, trust representation is the only one of the four that is discussed in detail in this paper.

### A. Trust representation

When looking at trust representation, it is important to note that we are looking at the way trust is represented from a holistic point of view. We are not interested in specific variables, their values and storage mechanisms. Rather we are looking at broader concepts that later influence specific trust representation, development and working thereof. Specific concepts include a trust outlook, passionate versus rational trust, centralized versus decentralized trust, trust versus distrust and trust scalability.

1) *Trust Outlook*: An agent's trust outlook refers to an agent's disposition to trust. This further refers to the extent to which an agent is willing to depend on another given specific context [10]. An agent's trust outlook influences the

means in which a trust value is developed and maintained. Jonker and Treur [9] have identified six means which define an agent's trust outlook. These are defined as follows:

*Blindly positive:* A blindly positive agent starts from a low trust value and looks for positive experiences with other agents. Once it reaches unconditional trust it remains there indefinitely. Unconditional trust is a state in which an agent trusts another unconditionally and does not limit the interactions participated in. Only positive experiences are evaluated and used to increase the trust value. Negative experiences are ignored.

*Blindly negative:* A blindly negative agent is the mirror case of the blindly positive one, starting from a high trust value for other agents and dropping the trust value as a result of negative experiences. Once it reaches unconditional distrust it remains there indefinitely. Unconditional distrust is a state in which an agent completely distrusts another and under no circumstances will participate in any interactions with that agent. Only negative experiences are evaluated and used to decrease the trust value. Positive experiences are ignored.

*Slow positive, fast negative:* An agent uses several positive experiences to build trust but can lose trust very easily with only a few negative trust experiences. For instance positive experiences will cause trust to increase by only one degree and negative experiences will cause a decrease in trust by only two degrees.

*Slow negative, fast positive:* Trust is built based on only a few positive experiences but several negative experiences are required in order to lose trust. For instance positive experiences will cause trust to increase by two degrees and negative experiences will cause a decrease in trust by only one degree.

*Balanced slow:* Allowing for slow update of trust in both the positive and negative domains. Trust will be increased or decreased in small degrees after thorough evaluation.

*Balanced fast:* Allowing for fast update of trust in both the positive and negative domains. Any change in trust will drastically influence a trust level in both a negative and positive manner.

These six approaches can be grouped under three main trust outlook approaches: optimism, pessimism and pragmatism. An optimistic agent expects good outcomes while a pessimistic agent expects the worst. A pragmatic agent exists somewhere in the spectrum between a pessimistic agent and an optimistic agent balancing positive and negative experiences [1]. The blindly positive as well as the slow negative, fast positive approaches are optimistic while the blindly negative and slow positive, fast negative are pessimistic. The balanced approaches are pragmatic.

Optimistic agents may present a system with more opportunities for interactions but also open a system up to greater risk. Pessimistic agents may lower risk exposure, but it may risk closing the system off from opportunities when the reason for failure is only temporary. Pragmatic agents lie somewhere in-between. The particular trust outlook that is considered best depends on the system the model is implemented in. A system that does not need to look for new opportunities and where the repercussions of a mistake are rather large and critical, such as in Internet banking, may prefer to take a pessimistic approach to trust.

2) *Passionate versus rational trust:* Passionate agents are considered to have a free will and thus act in a very human-

like manner. A passionate agent is expected to either be benevolent (an agent that behaves in an honest manner and follows the expected rules) or malicious (an agent that is deliberately dishonest and sets out to cause harm, hiding its intent to do so). Passionate agents develop trust according to intangible principles, or rather principles that have no specific binding mathematical rules attached to them. These principles include trust through collaboration, experience, reputation and recommendation and have varying mathematical definitions among various trust model implementations.

Rational agents are system-like agents. These agents are governed by a specific set of rules that tend to remain static. A rational agent lacks free will and is not expected to be benevolent or malicious. When trusting a rational agent it is expected that it will resist attempts of malicious manipulation from other agents [11]. The most common rational agent, is that of a firewall which grants and denies access according to fixed mathematical parameters that have been defined. Rational agents provide more control over interactions while passionate agents are given more freedom. Passionate agents are more adaptable than rational ones but also tend to expose a system to higher risk with higher potential gain. A passionate agent has a dynamic trust level for other agents. This level is increased and decreased over time and as a result of experiences. Unlike a firewall, a passionate agent will have varying trust levels over time. Depending on experiences and information gathered it grants access rights according to this dynamic trust level.

3) *Centralized versus decentralized trust:* Trust structures can either be centralized or decentralized [3]. Centralized structures allow a single centralized node to gather information from all other agents involved in an interaction. This node manages the interaction and ensures that all parties concerned abide by the same trust definitions. For instance, when defining trust using reputation, information is made globally visible, and defined by the entire system. Agents are allowed to influence one another's reputations by providing satisfaction feedback. A satisfaction feedback is feedback in which an agent indicates their level of satisfaction with a particular interaction. The feedback impacts other agents' reputation, which is stored in a single place and defines a new trust level for a particular agent.

Decentralized systems are a bit more involved in the trust establishment process than centralized nodes. Trust is subjective and established by each and every agent for other agents. Thus, agents' trust levels in others will vary from agent to agent dependent on each individual subjective context. Reputation is not global and the process of acquiring a reputation requires an agent to query other agents and combine the results received in order to obtain a global estimate. This form of establishing trust requires a high communication overhead.

In a centralized model, such as eBay, every agent has the same opinion as the central agent. eBay has a central agent that gathers all reputation based information. All agents looking for trust related information gather this information from this central source. Thus trust is global and every agent has the same trust value for another. In a decentralized approach, every agent has its own unique trust value based on the trust model in place [12]. Agents in a decentralized environment, such as ad-hoc environments [2] often do not

have a stable central source of information. Thus a decentralized approach is taken. Every agent determines a trust value for another according to their own rules and perceptions.

4) *Trust versus distrust*: Many trust models use a single value over a specific range in order to represent trust. This value is known as a trust value. For instance, values in the range between -1 and 1 are used to represent trust, 1 representing trust in another and -1 representing distrust.

This representation is simple and can be rather effective but has a very interesting problem. Does the -1 value represent distrust as a result of negative experiences or simply distrust based on lack of prior experience and knowledge [13]? This problem is further demonstrated by the uncertainty problem in ad-hoc environments. In environments with high mobility, such as ad-hoc networks, being uncertain about another node's trustworthiness is a common phenomenon [2], making it vital to distinguish between distrust and simple uncertainty. Modeling distrust as a separate parameter has been recommended to solve this problem.

A means of dealing with the uncertainty versus distrust problem has been proposed by Li, Lyu and Liu [2]. They recommend that trust representation is a 3-dimensional metric that includes values for trust, distrust as well as uncertainty. In order to successfully weigh trust against distrust, both positive and negative experiences are recorded. Positive experiences influence the trust parameter and negative values influence the distrust parameter. A trust value is ascertained as a combination of the two.

When working with values of distrust, it is important to keep in mind the fact that generally negative behaviour has more incentive to impact trust than positive behaviour. An interesting quote by Gambetta [14] summarizes this phenomenon rather nicely:

“While it is never that difficult to find evidence of untrustworthy behaviour, it is virtually impossible to prove its mirror image.”

Once distrust has been established it is often difficult to regain trust [1]. Thus, when working with parameters that indicate distrust, a trust model needs a means of addressing this issue in order for the evaluation to be accurate.

5) *Trust scalability*: As in any implementation, an important factor to take into consideration is the scale on which a trust model is expected to work [15]. Most authors do not address the scalability of their models [4], [5], [12], [16], thus requiring a little deductive reasoning when analysing their models for scalability. There are a few basic factors that can be taken into consideration when considering the scalability of a trust model.

Scalability deals with processing, network and space constraints that a particular system has. Experience and historical information are a good means of keeping a dynamic accurate trust value, but require space in which to store this information. This need for space can be curbed by allowing a trust model to only keep historical and experience-based information for only a short limited time period before overwriting old stale information with new information. Another means of saving space is to require an agent to only store such information about particular agents it may be interested in instead of all agents it may have encountered.

Another consideration is the networking capabilities of a particular environment. Some trust models require more messages to be exchanged than others incurring a higher network load. The more complex a trust representation is, the more likely it is that a higher message load will be required in order to successfully establish a trust relationship.

Some trust model implementations require agents to keep a list of friends, trusted nodes, trusted recommenders and even information about other nodes. The degree to which storage of this information is required, as well as possible overhead among agents, needs to be taken into consideration. Though not likely to pose a problem in small systems, space constraints can become an issue in large systems. Model's such as Abdul-Rahman and Hailes' Trust-Reputation model [16], that are required to store vast quantities of data are not very scalable. This model requires the storage of experience as well as recommendation information by each agent about all other agents it has encountered in an environment as well as the contexts in which this information was gathered.

Trust representation influences all the other categories of trust criteria defined by the author as it defines how information looks and flows. Only a brief description of the other three categories follows due to limited space constraints.

#### *B. Initial trust*

Initial trust refers to the strategy a trust model adopts in order to obtain an initial trust value for another agent in the environment. There are several strategies that can be chosen and used. These include but are not limited to recommendation, reputation, observation, institution, collaboration, negotiation and experience [1], [4], [5], [9], [12], [13], [14]. All of these require that the model gather some form of information in order to establish a trust value before participating in an interaction with another agent.

#### *C. Updating trust*

Due to the dynamic, ever-changing nature of trust, it is important to have a means of updating trust values. This allows an agent to change a trust value over time in order to keep up with changing environmental and situational factors. Agents are, thus, able to protect themselves from other agents that used to be trustworthy but became malicious over time. Often trust is updated using the same mechanisms that were used to define initial trust though there are a few additional factors that need to be taken into consideration. These are the influences of direct experience, feedback and transaction analysis.

#### *D. Evaluation of trust*

In order to successfully update trust, a trust model needs a means of evaluating the information it has gathered. Although several trust models use mechanisms that are closely linked to the means in which trust is initially established and updated in order to evaluate their trust values, there are additional strategies that are in use in order to evaluate trust and limit interactions. These include the use of roles and categorization. When evaluating a particular interaction, there are certain factors that need to be taken into consideration if an accurate analysis is to be obtained. These include the context in which an interaction occurred, the possible reasons for failure, the risk that was involved

and whether a dynamic or approximate computation is desired.

These four broad criteria categories have been proposed in order to ease analysis of currently proposed trust models. The next section demonstrates how this analysis process works for trust representation. An existing trust model is chosen and analysed using various points within the trust representation criteria category.

#### IV. EXAMPLE ANALYSIS OF TRUST REPRESENTATION

The trust model chosen in order to demonstrate a sample analysis using trust representation is Abdul-Rahman and Hailes' Trust-Reputation model [16]. This model was chosen due to its relative simplicity and inclusion of many of the concepts discussed. This model determines the trustworthiness of other agents based on collected statistics that include direct experiences and recommendations.

A set of direct experiences and recommendations is summarized in order to obtain a trust value. Experiences are recorded into two separate sets in order to be able to differentiate those that are a result of direct trust and those that are linked to recommendation. This way an agent is able to keep track of the direct trust it has in others as well as the trust level it has in recommendations from other agents.

In order to obtain a trust value for a particular agent in a particular context, this model relies on a basic system of counters. For every agent within a specific context, an agent possesses four counters. These counters are for varying trust degrees. The four counters this model makes use of are counters or very good, good, bad and very bad. Hence, these counters represent various trust levels namely very trustworthy, trustworthy, untrustworthy and very untrustworthy respectively. These counters are incremented with direct experiences an agent has as well as with recommendations an agent receives. The trust model runs a max function on these four counters that return the counter that has the largest value for the specific agent in a specific context. The trust counter with the largest value indicates the trust level that is to be assigned.

It is important to note that this model incorporates the concept of varying perception. Because trust is a subjective concept, it is logical to assume that perception of trust will differ among different agents. What one agent may define as trustworthy could be seen as untrustworthy by another agent based simply on differing perceptions.

This model allows for an agent to adjust recommendation values it receives from other agents in order to include the difference in perception. In order to accomplish this, an agent obtains an adjustment value. In order to obtain this adjustment value, an agent compares its own trust evaluation result for a particular agent in a particular context with the trust evaluation result of the recommender agent for the same agent in the same context. If the trust evaluation result differs, the agent creates an adjustment value for recommendations coming from that particular recommender.

For example, agent A is looking for an adjustment value for recommender B. Agent A knows that the trust value it has for agent D is 't' (trustworthy) in context C. A receives information from B that B's trust value for D in context C is 'vt' (very trustworthy). In other words, A's value for agent

D in the same context as B's value for the same agent is one level lower than B's. The adjustment value that A obtains will be -1. This value is then used to lower the trust value of all recommendations coming from agent B by 1 in order to more closely represent A's own perceptions.

This trust model is analysed using the concepts discussed under the trust representation section as follows.

*Trust Outlook:* The agents in this trust model have a rather pragmatic approach keeping a record of both positive and negative experiences in order to balance them in given contexts. Agents possess four experience counters: very good, good, bad and very bad that are incremented with direct experiences and recommendation information. Good experiences increment the good counter; very good experiences increment the very good counter and so forth. When determining a trust value a max function returns the highest count. Trust is assigned according to which counter has the highest count. If the max function returns more than one of the counters, an uncertainty value is assigned.

*Passionate versus Rational:* This model takes on a passionate approach, incorporating a mechanism of social control that clusters towards results that are positively reputable. The social concept this model builds on is that of reputation and recommendation, relying on the 'opinions' of other agents to make trust based decisions.

*Centralized versus Decentralized:* This model is decentralized. It is proposed for open distributed systems. There is no central agent that gathers all the information. Each agent has its own evaluations for others and is even allowed to adjust trust values it has received as recommendations.

*Trust versus Distrust:* While there are no explicit variable defined in order to handle distrust, an agent can differentiate between lack of trust due to lack of knowledge and lack of trust due to experiences and information it has gathered. An agent keeps an experience set for each agent it has interacted with and the context it has interacted in. This set has a counter value for very good, good, bad and very bad experiences. These values are incremented with experiences gained.

*Scalability:* The model keeps the format of the information that an agent needs to store rather simple. Although, it does not require a lot of space to store information about a single agent in a single context, this model still has scalability issues due to space constraints. The model does not limit the number of agents, or the number of contexts or even the period of time for which experience information is gathered and stored. Should these issues remain unaddressed; this model will encounter scalability issues due to the sheer number of records the agent is expected to keep seeing as agents store trust information in agent context pairs.

#### V. DISCUSSION

This paper addresses the problem of analysing various trust models in order to determine the efficiency of a trust model and pinpoint issues that have not been addressed. Four main categories of criteria have been identified by the author. These categories define the main features any good trust model is required to have. The main categories identified are trust representation, initial trust, updating trust and trust evaluation.

Due to space constraints, only one of the four criteria categories is discussed in detail. The chosen category is that of trust representation. Trust evaluation is covered in another paper submitted by the author for review [17]. This particular category was chosen because of its importance. Trust representation influences later the means in which initial trust is established, trust is updated and trust is evaluated. The latter three have not been addressed in this paper in detail. Factors influencing the means in which trust is represented that have been identified and discussed in this paper include trust outlook, passionate versus rational trust, centralized versus decentralized trust, weighing trust against distrust and the scalability of a model.

## VI. CONCLUSION

This paper introduced and discussed the concept of a set of criteria that is to be used for the evaluation of trust models. These criteria are intended to be a guideline to trust model evaluation in order to identify the efficiency of a particular trust model. In the same way that they can be used to evaluate a currently implemented trust model, they can also be used as a guide for factors and issues to take into consideration for future trust model implementations.

Using these criteria, one is able to identify how a trust model addresses certain issues and also which issues have not been addressed. An example of such an issue is the scalability issue that was not successfully addressed by Abdul-Rahman and Hailes' model above. This is important knowledge to have when considering choosing a particular trust model for implementation and can also be used to guide future improvements on trust model architectures.

Abdul-Rahman and Haile's Trust-Reputation model was taken as an example and analysed using the factors identified within the trust representation criteria category. It is important to realize that this criteria are not necessarily all the possible defined criteria that can be taken into consideration. They are based on 'known' issues and known implementations and it is possible to expand them in future work. Future work also includes the development of a measurement mechanism in order to score the degree to which a trust model addresses the issues identified.

## REFERENCES

- [1] Marsh, S.P. Formalising Trust as a Computational Concept. In Dissertation for the Department of Computing Science and Mathematics, University of Stirling. 1994.
- [2] Li, X. Lyu, M.R. & Liu, J.. A Trust Model Based Routing Protocol for Secure Ad Hoc Networks. In IEEE Aerospace Conference Proceedings.. 2004. ISSN: 0-7803-8155-6/041.
- [3] Wang, Y. & Vassileva, J. Bayesian Network-Based Trust Model. In Proceedings of Web Intelligence, 2004. WI 2004. IEEE/WIC?ACM International Conference on 20-24 Sept 2004. pp 341-348. ISSN: 0-7695-2100-2.
- [4] Azzedin, F. & Maheswaran, M. Trust Modeling for Peer-to-Peer Based Computing Systems. In Proceedings of the International Parallel and Distributed Processing Symposium. 2003.
- [5] Huynh, T.D., Jennings, N.R. & Shadbolt, N.R. FIRE: An Integrated Trust and Reputation Model for Open Multi-Agent Systems. In Proceedings of 16th European Conference on Artificial Intelligence, pp. 18-22, Valencia, Spain. 2004.
- [6] Nooteboom, B., (2002) Trust: Froms, Foundations, Functions, Failures, and Figures, Edward Elgar Publishing, Ltd.

- Cheltenham UK, Edward Elgar Publishing, Inc. Massachusetts, USA, ISBN: 1 84064 545 8.
- [7] Golembiewski, Robert T., & McConkie, Mark. 1975. The Centrality of Interpersonal Trust in Group Processes. Chap. 7, pages 131–185 of: Cooper, Cary L. (ed), Theories of Group Processes. Wiley.
- [8] Pirzada, A.A. & McDonald, C. Establishing Trust in Pure Ad-hoc Networks. In Research and Practice in Information Technology. Vol. 26 V. Estivill-Castro, Ed. 2004.
- [9] Abdul Jonker C.M. & Treur J. 1999. Formal Analysis of Models for the Dynamics of Trust based on Experiences. In Modelling Autonomous Agents in a Multi-Agent World, pp 221-231. 1999.
- [10] Li, X., Valacich, J.S. & Hess, T.J. Predicting User Trust in Information Systems: A Comparison of Competing Trust Models. In Proceedings of the 37th Hawaii International Conference on Systems Sciences. 2004.
- [11] Josang, A. The right type of trust for distributed systems. In C. Meadows, editor, Proc. of the 1996 New Security Paradigms Workshop. ACM, 1996.
- [12] Liang, Z. & Weisong, S. PET: A PERSONALIZED TRUST MODEL WITH REPUTATION AND RISK EVALUATION FOR P2P RESOURCE SHARING. In Proceedings of the 38th Hawaii International Conference on Systems Sciences. 2005.
- [13] Guha, R., Kumar, R., Raghaven, P. & Tomkins, A. Propagation of Trust and Distrust. In Proceedings of the Thirteenth International World Wide Web Conference, 2004.
- [14] Gambetta, Diego. 1990. Can we Trust Trust? Chap. 13, pages 213–237 of: Gambetta, Diego (ed), Trust. Blackwell.
- [15] Luo, H., Zerfos, P., Kong, J., Lu, S. & Zhang, L. Self-securing Ad Hoc Wireless Networks. In: Seventh IEEE Symposium on Computers and Communications (ISCC). 20021.
- [16] Abdul-Rahman, A. & Hailes, S. Relying on Trust To Find Reliable Information. In Proceedings of DWACOS'99, Baden-Baden, Germany., 1999.
- [17] Wojcik, M., Venter, H.S. & Eloff, J.H.P Trust Model Evaluation Criteria: A Detailed Analysis of Trust Evaluation. Submitted for review for ISSA 2006.

**Marika Wojcik** was born in Carletonville, South Africa in 1982. Obtained a B.Sc. IT Information and Knowledge Systems degree (2003) and a B.Sc. (Hons.) Computer Science degree (2004) from the University of Pretoria. Is currently studying for a M.Sc majoring in Computer Science at the University of Pretoria.